Mise en place d'un SSO

Objectifs de cette séquence d'exercices :

- Expliquer le concept d'un SSO, fonctionnement, protocoles utilisés, acteurs participants au processus.
- Implémenter un server SSO pour l'authentification d'un extranet.

Console à utiliser :

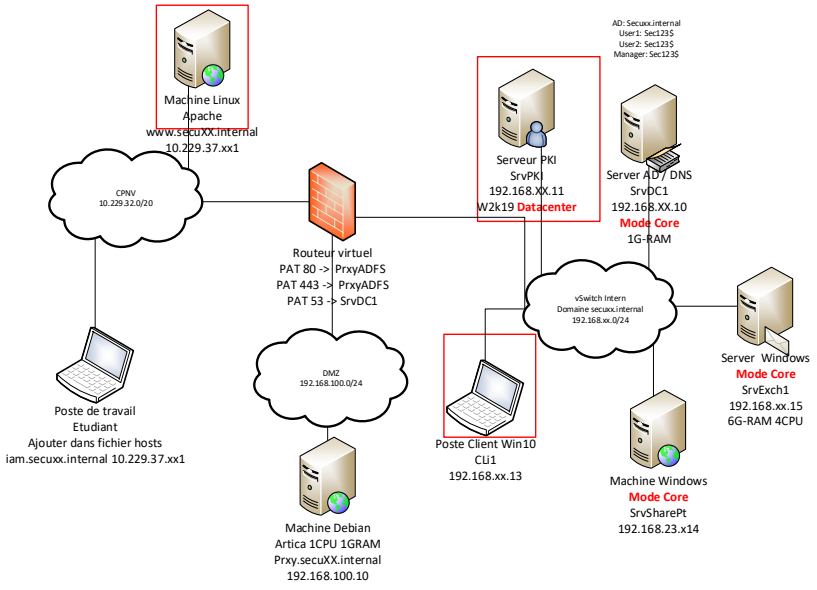
- Outil ssh : `putty.exe`
- Outils de configuration Active Directory Federation Service: `Microsoft.IdentityServer.msc` (il faut au-préalable ajouter le service)

Documents/fichiers :

Sous linux, pour une meilleure compatibilité, préférer l'installation par paquet plutôt que l'installation en téléchargeant les sources (Exemple : sudo apt-get install simplesamlphp ou yum install simplesamlphp

- http://arnaudpain.com/2019/08/05/windows-server-2019-adfs-step-by-step/#sthash.8LKvGLb2.dpbs
- https://techexpert.tips/fr/simplesamlphp-fr/simplesamlphp-installation-sur-ubuntu-linux/
- http://www.lewisroberts.com/2015/09/06/integrating-simplesamlphp-with-adfs-2012r2/
- http://anthonyreault.free.fr/Veille/Sso/co/SSO_10.html
- https://www.codeflow.site/fr/article/how-to-install-and-configure-simplesamlphp-for-saml-authentication-on-ubuntu-16-04
- https://docs.microsoft.com/en-us/azure/active-directory/saas-apps/saml-toolkit-tutorial
- http://www.mikrotikminute.com/how-to-do-a-packet-capture-with-mikrotik-routers-part-1/

Schéma :
Machines nécessaires pour le module sont entourées en rouge



1 – Analyse infrastructure:

Concept d'une authentification centralisée de type SSO

- Définir le concept d'un SSO
- Dans le cadre du SSO, définir les notions de : service provider, identity provider
- Définir le fonctionnement d'un SSO
- Définir les protocoles utilisés, ainsi que les utilisations
- Trouver deux implémentations de SSO et exposer les avantages et inconvénient de ces solutions.

2 – Mise en place du server SSO:

Mettre en place le serveur ADFS sur la machine Serveur PKI (SrvPKI) et démontrer l'utilisation du SSO à l'aide de l'implémentation de simplesamlphp sur la machine Extranet (www.secuxx.internal), voir l'URL dans documents/fichiers
Dans un premier temps laisser les requêtes d'authentification traverser le pare-feu jusqu'au serveur ADFS.

Cahier des charges :

10. En tant que responsable de la sécurité, je veux que les utilisateurs de mon infrastructure puissent se logger avec un compte de l'AD sur l'extranet qui se trouve sur la machine www.secuxx.internal, dans le but que les utilisateurs aient qu'un seul compte d'accès pour l'extranet et l'AD.
11. En tant que responsable de la sécurité, je veux que lorsque les utilisateurs de mon infrastructure se logge avec un compte de l'AD sur l'extranet, que l'ensemble des transactions soient sécurisées, dans le but de garantir la confidentialité à mes utilisateurs.
12. En tant que responsable de la sécurité, je veux que le flux d'authentification passe par un reverse proxy dans la DMZ, dans le but de sécurisé les requêtes qui sont envoyées aux serveurs ADFS dans le LAN (optionnel).

4 – Rapport de mise en service :

Rédiger un rapport de mise en services avec les points ci-dessous.

- Schéma à jour
- Copie d'écran des divers SP sur simplesamlphp
- Montrer la redirection sur l'IdP
- Le retour du token
- Le fonctionnement de l'extranet développé par vousMontrer les divers Relaying Partie Trust (approbation de partie de confiance) de l'ADFS
- Montrer l'onglet Encryption de l'approbation de confiance
- Montrer une capture Wireshark de l'échange de tocken
- Montrer la liste des certificats dans la rubrique Service de l'ADFS